Optimal detection to improve the performance of two-hop routing in selfish OppNets

A, B, C
School of Cyber Sci. & Engr., Southeast University, Nanjing, China
Key Lab of CNII, MOE, Southeast University, Nanjing, China
Jiangsu Provincial Key Laboratory of Computer Network Technology, Southeast University, Nanjing, China

***Index Terms*—OppNet, Selfish, Black (Gray) Hole, ODE, Pontryagain's maximal principle**

I. Introduction

II. Related Work

A. Selfish OppNets

Observing the importance of OppNets over traditional networks for exchanging information, much efforts has been made to explore the OppNets with selfish nodes in the past few years. The majority of existing studies focus on selfish node detection(or misbehavior detection), for the behavior of selfish nodes may cause vulnerability and decrease the performance of OppNets, which was verified and numerical results were given in [1]. Most selfish node detection approaches can be broadly classified into two groups-the first groups relies on watchdog systems and the other depends on social trust-based communications [2].

For example, [3] [4] both proposed a collaborative watchdog approach based on the diffusion of selfish nodes awareness. [5] proposed a social-based watchdog system(SoWatch) for selfish nodes detection. Compared to most of existing detection schemes that primariliy rely on the nodes' contact records, SoWatch takes nodes' individual and social preferences into account. Zhu et al. proposed a probabilistic misbehavior detection scheme(iTrust) to judge a node's behavior, based on the collected routing evidences and probabilistically checking in [6]. A metric of misbehavior(MoM) for mathematically evaluating the extent of misbehavior of a node was introduced in [7], in which the misbehaving nodes were considered as the voting alternatives and the normally behaving nodes as the voters based on the Theory of Social Choice. A "Friendship and Selfishness Forwarding"(FSF) algorithm for accessing the relay node's selfishness was presented in [8], with the consideration of the friendship strength among a pair of nodes by using a machine learning algorithm. [9] proposed a provenance-based trust framework that aims to achieve accurate peer-to-peer trust assessment. Except approaches mentioned above that belong to the two classes, researchers also investigated other methods to improve selfish node detection. Basu et al. combined watchdog technique with trust-based communications and integrated with PRoPHET to build a global perception of forwarding behavior for detection of selfish nodes in [10]. Devi V. et al. introduced Semi Markov

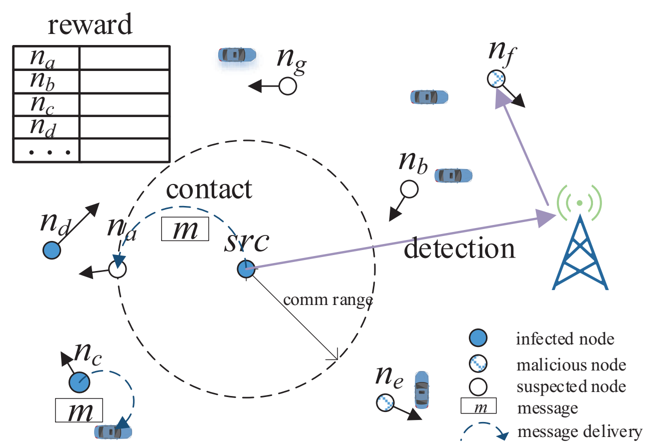

Fig. 1: Reward and Detection of the selfish nodes in OppNets.

process for quantifying and future forecasting the probability with which the node could turn into selfish in WSN in [11].

Routing is a critical bottleneck after selfish nodes are detected and many literatures designed their routing algorithms for selfish OppNets with incentive mechanisms [12] [13] [14] [15] [16]. For instance, Li et al. proposed an incentive aware routing for selfish OppNets from a game theoretic perspective, which jointly considered individual selfishness and social selfishness to improve the performance of OppNets in [14]. What's more, Energy-aware routing schemes were presented in [17] [18]. Mao et al. investigated the energy-aware routing problem in MANETs with nodes'selfishness and solution based on game theory was given in [17]. Wu et al. proposed an energy-efficient copy-limit-optimized algorithm for epidemic routing in multi-community scenarios with social selfishness considerations using the Ordinary Differential Equations(ODEs) in [18]. [19] proposed a routing algorithm based on Geographic Information and Node Selfishness, which combines nodes' willingness to forward and their geographic information to maximize the possibility of contacting the destination.

III. Preliminaries

The source node src needs to disseminate its message m to vehicles or pedestrians. The N relay nodes can replicate m and send it to the vehicles, which is shown in Fig. 1. Thus the potential coverage area of the message is broadened by

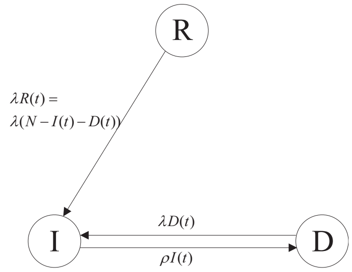

Fig. 2: State transition of the relay nodes without detection.

the opportunistic network. To encourage the collaboration of relay nodes, src should reward the relay node n_i $(1 \leq i \leq N)$ based on the time, when the message are carried by n_i. The time ranges from the replication time (τ_i) to the time-to-live of the message (T). τ_i can be recorded by src when n_i contacts src and replicates m. However, n_i may discard m immediately after the contact to earn the reward without carrying m, which is the selfish behavior. So src can check the checksum of m's specific part, which is store in the randomly selected relay node n_i. If the check failed, n_i will be identified as the selfish node and can not receive the reward. In this paper, we propose the optimal randomly detection strategy to achieve the tradeoff between the cost of the random detections and the wasted reward of the selfish behaviors.

$E(R(t))$ denotes the expected number of the relay nodes, which have not contacted src before time t. $E(I(t))$ denotes the expected number of infected relay nodes, which still carry the message at time t. $E(D(t))$ denotes the expected number of selfish relay nodes, which have discarded the message but are not known by src at time t. Similar to [20] and [21], the contacts between each pair of nodes including src are assumed to occur according to the Poisson process, in which the contact rate is λ. The total number of relay nodes is N, and $N = R(t) + I(t) + D(t)$, $\forall t$, $0 \leq t \leq T$. We also assume the change rate of becoming the selfish node is a constant value ρ. The detection rate is $U(t)$, $0 \leq U(t) \leq U_m$, $\forall t$, $0 \leq t \leq T$. which is the control function. To simplify the denotations, we use $R(t)$, $I(t)$ and $D(t)$ to replace $E(R(t))$, $E(I(t))$ and $E(D(t))$, respectively.

Then the main objective of our work is to solve the following problem,

$$Min : J = \int_0^T (1-\alpha)D(t) + \alpha U(t) dt,$$

IV. Construction of the ODE Model

We investigate the selfish detection in this and the following sections. Specifically, in this section, the ordinary differential equation model is constructed to capture the state change with time.

A. Without Detection

First, we analyze the change of the network state with time when the selfish detection is not deployed. The state transition is shown in Fig. 2 with the following rules. The nodes change from state R to state I if they contact src. The corresponding incremental rate of state I is $\lambda R(t)$ at time t. The selfish node also may contact src in the opportunistic network. Then the total incremental rate of I is $\lambda(R(t) + D(t)) = \lambda(N - I(t))$. Additionally, the infected node may become the selfish node with rate ρ. Thus we can obtain the derivative of $I(t)$ with respect to t,

$$\frac{\mathrm{d}I(t)}{\mathrm{d}t} = \lambda(N - I(t)) - \rho I(t).$$

where λ and ρ are constants. Similar to $\frac{\mathrm{d}I(t)}{\mathrm{d}t}$, we can get the change rate of state D and state R, i.e. $\frac{\mathrm{d}D(t)}{\mathrm{d}t}$ and $\frac{\mathrm{d}R(t)}{\mathrm{d}t}$, and obtain the model,

$$\begin{aligned} \frac{\mathrm{d}I(t)}{\mathrm{d}t} &= \lambda(N - I(t)) - \rho I(t), \\ \frac{\mathrm{d}D(t)}{\mathrm{d}t} &= -\lambda D(t) + \rho I(t), \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} &= -\lambda(N - I(t) - D(t)), \end{aligned} \tag{1}$$

Since (1) is formed by the first-order first-power ordinary differential equations, we can calculate the general solutions of it, that is.

$$I(t) = Ce^{-(\lambda+\rho)t} + \frac{\lambda N}{\lambda + \rho}.$$

At first, $M(0) = 0$ and $I(0) = 0$, only src has the messages. Note that $0 \leq I(t) \leq N$ and $0 \leq M(t) \leq N$. We use $\dot{I}$ and $\dot{M}$ denote $I(t)$ and $M(t)$. Following the two-hop routing, where only the source node can replicate the message to other nodes, we get that the corresponding ODEs like [21], which are

when $0 \leq I(t) \leq N$ and $0 \leq M(t) \leq N$.

And then we find the close-form value of $I(t)$ and $M(t)$ to ensure I_s and M_s. From the first ODE, $\dot{I} + \rho I = \beta(N - I)$, we can obtain

Considering that $I(t = 0) = 0$, $C = \frac{-\beta N}{\beta + \rho}$. Thus

$$I(t) = \frac{\beta N}{\beta + \rho} - \frac{\beta N}{\beta + \rho} e^{-(\beta+\rho)t}.$$

Similarly, from $\dot{M} + \beta M = \rho I$,

$$\begin{aligned} M(t) &= Ce^{-\int \beta dt} + e^{-\int \beta dt} \int \rho I e^{\int \beta dt} dt \\ &= Ce^{-\beta t} + e^{-\beta t} \int \rho \frac{\beta N}{\beta + \rho}(1 - e^{-(\beta+\rho)t}) e^{\beta t} dt \\ &= Ce^{-\beta t} + \frac{\beta N}{\beta + \rho} e^{-(\beta+\rho)t} + \frac{\rho N}{\beta + \rho} \end{aligned}$$

Because of $M(0) = 0$,

$$M(t) = -Ne^{-\beta t} + \frac{\beta N}{\beta + \rho} e^{-(\beta+\rho)t} + \frac{\rho N}{\beta + \rho}$$

We can find that when $t \to +\infty$, $I(t) \to \frac{\beta N}{\beta + \rho}$ and $M(t) \to \frac{\rho N}{\beta + \rho}$.

B. Object Function

The expected number of nodes, which declare that holding the messages, in the range $t \in (0, T]$ can be viewed as the contribution of the relay nodes, which will be proportional to the reward paid from the message sender. Thus the total paid reward for the selfish behaviors is

$$J = \int_0^T M(t) dt,$$

where T is the Time to Live (TTL) of message m. $M(t)$ is the waste of the reward at the instant time t. which also can

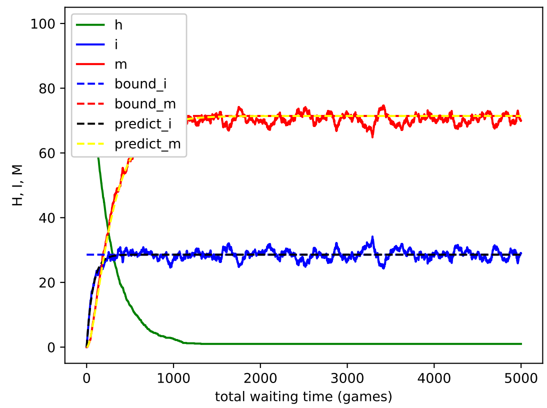

Fig. 3: $I(t)$ and $M(t)$ with time t obtained from prediction and simulations when $\beta = 0.004$, $\rho = 0.01$ and $N = 100$. Here h and i is the mean value of 20 simulations.

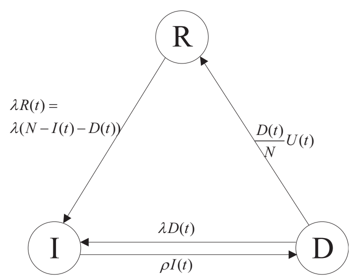

Fig. 4: State transition of the relay nodes.

be calculated. Based on the calculated result, We can find that ()% reward are paid to the nodes without messages.

V. Full detection in two-hop routing

The detection rate is U_m. For each detection, a node will be chosen randomly from N nodes. Thus the probability that find the blackhole node is $\frac{M}{N}$.

$$\dot{I} = \beta(N - I) - \rho I,$$
$$\dot{M} = \rho I - \beta M - \frac{M}{N}U_m,$$
$$\dot{S} = -\beta(N - I - M) + \frac{M}{N}U_m,$$

So

$$I(t) = \frac{\beta N}{\beta+\rho} - \frac{\beta N}{\beta+\rho}e^{-(\beta+\rho)t},$$

Then

$$\dot{M} + (\beta + \frac{U_m}{N})M = \rho I$$

$$\begin{aligned}
&M(t)\\
=&Ce^{\int -(\beta+\frac{U_m}{N})dt} + e^{\int -(\beta+\frac{U_m}{N})dt}\int \rho I e^{\int(\beta+\frac{U_m}{N})dt}dt\\
=&Ce^{-(\beta+\frac{U_m}{N})t} + e^{-(\beta+\frac{U_m}{N})t}\rho\frac{\beta N}{\beta+\rho}\int(1-e^{-(\beta+\rho)t})e^{(\beta+\frac{U_m}{N})t}dt\\
=&Ce^{-(\beta+\frac{U_m}{N})t} + \frac{\rho\beta N}{\beta+\rho}\frac{1}{\beta+\frac{U_m}{N}} - \frac{\rho\beta N}{\beta+\rho}\frac{1}{\frac{U_m}{N}-\rho}e^{-(\beta+\rho)t}
\end{aligned}$$

Because of $M(0) = 0$.

$$\begin{aligned}
M(t) =&\frac{\rho\beta N}{\beta+\rho}\frac{1}{\beta+\frac{U_m}{N}} - \frac{\rho\beta N}{(\beta+\frac{U_m}{N})(\frac{U_m}{N}-\rho)}e^{-(\beta+\frac{U_m}{N})t}\\
&-\frac{\rho\beta N}{\beta+\rho}\frac{1}{\frac{U_m}{N}-\rho}e^{-(\beta+\rho)t}
\end{aligned}$$

Here we find that ()% reward is wasted in the selfish node. Although the wasted reward is reduced because of the detection, the additional cost, which is caused by the detection behavior, i.e., energy, bandwidth and wireless communication charge. is introduced.

VI. Optimal Detection

A. Problem Formulation

Assume that the detection can be conducted. The detection rate is $U(t)$, $0 \leq U(t) \leq U_m$. U_m is the limitation of the detection rate, which is the constraint from the hardware and the time sequences. We also use $\dot{U}$ to denote $U(t)$. Then, the ODEs can be reformed as

$$\begin{aligned}
\dot{I} &= \beta(N - I) - \rho I,\\
\dot{M} &= \rho I - \beta M - \frac{M}{N}U,\\
\dot{S} &= -\beta(N - I - M) + \frac{M}{N}U.
\end{aligned} \tag{2}$$

Meanwhile,

$$\begin{aligned}
I(0) &= 0,\\
M(0) &= 0,\\
S(0) &= N.
\end{aligned} \tag{3}$$

Thus $I(t)$ is the same with that in the situation without detection, which is

$$I(t) = \frac{\beta N}{\beta+\rho} - \frac{\beta N}{\beta+\rho}e^{-(\beta+\rho)t}. \tag{4}$$

Considering that the detection is also the cost, the object function will be

$$J = \int_0^T (1-\alpha)M + \alpha U dt.$$

Here α is the weight, which can control the importance between the cost of selfish relay nodes and detections. Thus $0 < \alpha < 1$. Similar with the previous section, $I(t)$ and $M(t)$ is the state variable. $U(t)$ is the controllable variable, $0 \leq U(t) \leq U_m$.

B. Optimal Control by Pontryagin's Maximal Principle

Now we utilize the Pontryagin's maximal principle to find the optimal $U(t)$, which will minimize the total cost. First, the Hamilton function is

$$\begin{aligned}
H =&(1-\alpha)M + \alpha U + \lambda_1(\beta(N-I) - \rho I)\\
&+ \lambda_2(\rho I - \beta M - \frac{M}{N}U)\\
=&(1-\alpha)M + \alpha U + \lambda_1(\beta(N-I) - \rho I) + \lambda_2\rho I\\
&- \beta\lambda_2 M - \lambda_2\frac{1}{N}UM\\
=&(1-\alpha)M + \lambda_1(\beta(N-I) - \rho I)\\
&+ \lambda_2(\rho I - \beta M) + (\alpha - \lambda_2\frac{M}{N})U.
\end{aligned}$$

Note that λ_1 and λ_2 denote $\lambda_1(t)$ and $\lambda_2(t)$, respectively. Without the final constraint, the terminal condition is $\lambda_2(T) = 0$ and $\lambda_3(T) = 0$. The adjoint function is

$$\dot{\lambda_2} = -\frac{\partial H}{\partial M} = \lambda_2(\beta + \frac{U}{N}) - (1-\alpha).$$

Thus

$$U^*(t) = \begin{cases} 0, & \text{if } \alpha - \lambda_2 \dfrac{M}{N} \geq 0 \\ U_m, & \text{if } \alpha - \lambda_2 \dfrac{M}{N} < 0 \end{cases} \tag{5}$$

In summary, we have the ODE functions $\dot{M}$, $\dot{\lambda_2}$, the initial condition $M(0) = 0$ and the boundary condition $\lambda_2(T) = 0$, Thus the problem is to solve a BVP problem, which is

$$\begin{aligned} \dot{M} &= \rho I - \beta M - \frac{M}{N}U, \\ \dot{\lambda_2} &= -\frac{\partial H}{\partial M} = \lambda_2(\beta + \frac{U}{N}) - (1-\alpha), \\ M(0) &= 0, \\ \lambda_2(T) &= 0. \end{aligned} \tag{6}$$

We can solve the BVP problem with the shooting method by the bvpSolve package of R.

VII. Analysis of Optimal Detection

In this section, we will introduce the properties of the optimal control variable.

Lemma 1. *At the beginning and the end of the whole duration, the optimal control stop the selfish detection, which is $U(0) = U(T) = 0$.*

Proof. At the beginning of the duration, $M(0) = 0$, which is the initial condition of 6. Then $\alpha - \lambda_2(0)\frac{M(0)}{N} = \alpha > 0$. Following (5), the optimal $U(0) = 0$.

At the end of the duration, $\lambda_2(T) = 0$, which is the boundary condition of 6. Then $\alpha - \lambda_2(T)\frac{M(T)}{N} = \alpha > 0$. Based on (5), the optimal $U(T) = 0$. □

Based on the differential function $\dot{I}$, the equilibrium point of I can be obtained from $\dot{I} = 0$, which is $I^* = \frac{\beta N}{\beta+\rho}$. When $I(t) < I^*$, $I(t)$ will increase with t and approach to $\frac{\beta N}{\beta+\rho}$. Meanwhile, in this paper $I(0) = 0$ at the beginning of time.

Based on the differential function $\dot{M}$, the equilibrium point is obtained from $\dot{M} = 0$, which is $M^* = \frac{\rho I}{\beta + \frac{1}{N}U}$. In the situation without detection, the equilibrium point is $M^* = \frac{\rho I^*}{\beta} = \frac{\rho N}{\beta+\rho}$. In the situation with full detection, the equilibrium point is $M^* = \frac{\rho I^*}{\beta+\frac{1}{N}U_m} = \frac{\rho}{\beta+\frac{1}{N}U_m}\frac{\beta N}{\beta+\rho}$.

Since α is the weight of detecting the selfish nodes, we can assume that if α is enough high, the detection will not perform according to the optimal control strategy.

Lemma 2. *If $\alpha \geq \alpha_{th}$, the optimal control let the detection stop in the whole duration, namely $U(t) = 0$, $0 \leq t \leq T$.*

Proof. Assume that ρ, N, β is given. Let $W(t) = \lambda_2(t)M(t)$.

$$\begin{aligned} W^{'}(t) =& M^{'}(t)\lambda_2(t) + M(t)\lambda_2^{'}(t) \\ =& (\rho I(t) - \beta M(t) - \frac{M(t)}{N}U(t))\lambda_2(t) \\ &+ M(t)(\lambda_2(t)(\beta + \frac{U(t)}{N}) - (1-\alpha)) \\ =& \rho\lambda_2(t)I(t) - (1-\alpha)M(t). \end{aligned} \tag{7}$$

Since $M(0) = 0$ and $\lambda_2(T) = 0$, $W(0) = W(T) = 0 < \alpha N$.

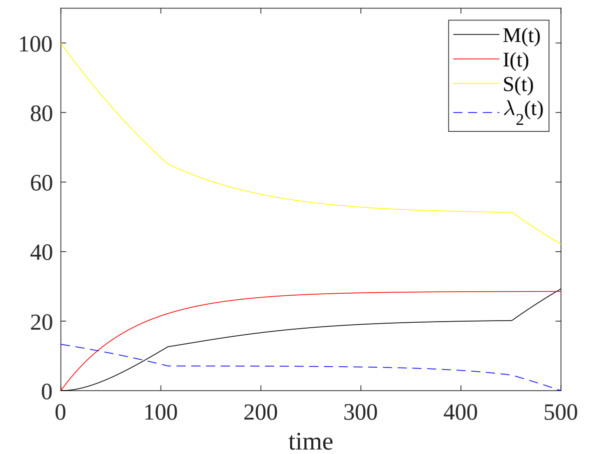

Fig. 5: State variable of analysis with time.

Now we focus on the poles of $W(t)$, namely t^*, where $W^{'}(t^*) = \rho\lambda_2(t^*)I(t^*) - (1-\alpha)M(t^*) = 0$. Then $M(t^*) = \frac{\rho\lambda_2(t^*)I(t^*)}{1-\alpha}$.

$$W(t^*) = \lambda_2(t^*)M(t^*) = \frac{\rho I(t^*)\lambda_2(t^*)^2}{1-\alpha}. \tag{8}$$

According to $\dot{\lambda_2}$ in (6), the equilibrium point of λ_2 is that $\lambda_2^* = \frac{1-\alpha}{\beta+\frac{U}{N}}$. Since $0 \leq U \leq U_m$, $0 < \frac{1-\alpha}{\beta+\frac{U_m}{N}} \leq \lambda_2^* \leq \frac{1-\alpha}{\beta}$. Note $\lambda_2(T) = 0$. Based on the phase line in ODE for $\dot{\lambda_2}$, $\lambda_2(t)$ decreases with t when $\lambda_2(t) < \lambda_2^*$. Conversely, $\lambda_2(t)$ increases with t when $\lambda_2(t) > \lambda_2^*$. Thus $0 \leq \lambda_2(t) \leq \lambda_2^* \leq \frac{1-\alpha}{\beta}$ when $0 \leq t \leq T$. Additionally, $0 \leq I(t) \leq \frac{\beta N}{\beta+\rho}$. From (8), we can derive that the upper boundary of $W(t)$, W_{up}, which is

$$W(t) \leq W(t^*) \leq \frac{\rho}{1-\alpha}\frac{\beta N}{\beta+\rho}(\frac{1-\alpha}{\beta})^2 = \frac{\rho N(1-\alpha)}{\beta(\beta+\rho)} = W_{up}.$$

Assume that α can satisfy that $W_{up} \leq \alpha N$, which means that $\alpha \geq \frac{\rho}{\beta(\beta+\rho)+\rho} = \alpha_{th}$. Then $W(t) \leq \alpha N$, when $0 \leq t \leq T$. Therefore the optimal control $U^*(t) \equiv 0$, when $0 \leq t \leq T$. □

VIII. Performance Evaluation

IX. Conclusion

References

[1] M. Karaliopoulos, "Assessing the vulnerability of DTN data relaying schemes to node selfishness," *IEEE Commun. Lett.*, vol. 13, no. 12, pp. 923–925, 2009. [Online]. Available: https://doi.org/10.1109/LCOMM.2009.12.091520

[2] B. Jedari, F. Xia, and Z. Ning, "A survey on human-centric communications in non-cooperative wireless relay networks," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 2, pp. 914–944, 2018. [Online]. Available: https://doi.org/10.1109/COMST.2018.2791428

[3] E. Hernández-Orallo, M. D. S. Olmos, J. Cano, C. M. T. Calafate, and P. Manzoni, "Evaluation of collaborative selfish node detection in MANETS and dtns," in *The 15th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, MSWiM '12, Paphos, Cyprus, October 21-25, 2012*, A. Y. Zomaya, B. Landfeldt, and R. Prakash, Eds. ACM, 2012, pp. 159–166. [Online]. Available: https://doi.org/10.1145/2387238.2387266

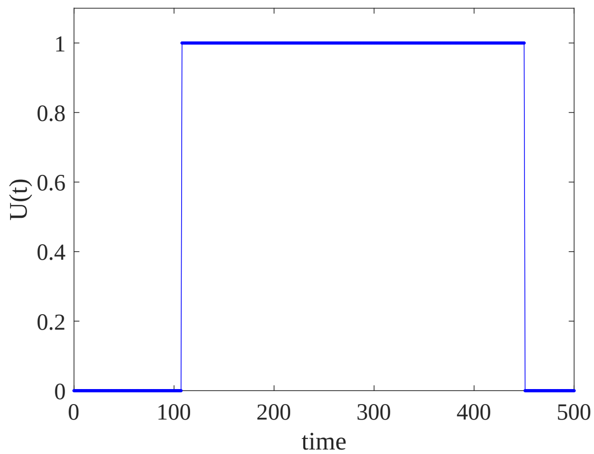

Fig. 6: Control variable of analysis with time.

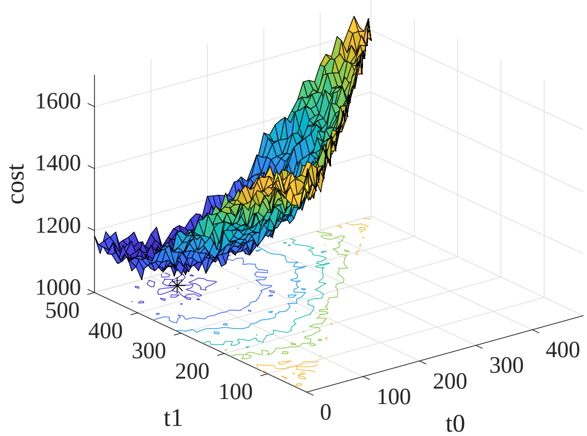

Fig. 7: Different choices of $t0$ and $t1$.

[4] E. Hernández-Orallo, M. D. S. Olmos, J. Cano, C. T. Calafate, and P. Manzoni, "Cocowa: A collaborative contact-based watchdog for detecting selfish nodes," *IEEE Trans. Mob. Comput.*, vol. 14, no. 6, pp. 1162–1175, 2015. [Online]. Available: https://doi.org/10.1109/TMC.2014.2343627

[5] B. Jedari, F. Xia, H. Chen, S. K. Das, A. Tolba, and Z. Al-Makhadmeh, "A social-based watchdog system to detect selfish nodes in opportunistic mobile networks," *Future Gener. Comput. Syst.*, vol. 92, pp. 777–788, 2019. [Online]. Available: https://doi.org/10.1016/j.future.2017.10.049

[6] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," *IEEE Trans. Parallel Distributed Syst.*, vol. 25, no. 1, pp. 22–32, 2014. [Online]. Available: https://doi.org/10.1109/TPDS.2013.36

[7] S. Chatterjee, S. Sarkar, and S. Misra, "Quantification of node misbehavior in wireless sensor networks: A social choice-based approach," in *IEEE International Conference on Communication, ICC 2015, London, United Kingdom, June 8-12, 2015, Workshop Proceedings*. IEEE, 2015, pp. 1479–1484. [Online]. Available: https://doi.org/10.1109/ICCW.2015.7247388

[8] C. B. Souza, E. Mota, L. Galvao, D. Soares, P. Manzoni, J. Cano, and C. T. Calafate, "Friendship and selfishness forwarding: applying machine learning techniques to opportunistic networks data forwarding," *CoRR*, vol. abs/1705.08808, 2017. [Online]. Available: http://arxiv.org/abs/1705.08808

[9] J. Cho and I. Chen, "PROVEST: provenance-based trust model for delay tolerant networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 1, pp. 151–165, 2018. [Online]. Available: https://doi.org/10.1109/TDSC.2016.2530705

[10] S. Basu, A. Biswas, S. Roy, and S. D. Bit, "Wise-prophet: A watchdog supervised prophet for reliable dissemination of post disaster situational information over smartphone based DTN," *J. Netw. Comput. Appl.*, vol. 109, pp. 11–23, 2018. [Online]. Available: https://doi.org/10.1016/j.jnca.2018.02.012

[11] K. D. V. and G. R., "Semi markov process inspired selfish aware co-operative scheme for wireless sensor networks (SMPISCS)," *Cybersecur.*, vol. 2, no. 1, p. 4, 2019. [Online]. Available: https://doi.org/10.1186/s42400-019-0021-3

[12] H. Wang, H. Wang, F. Guo, G. Feng, and H. Lv, "ARAG: A routing algorithm based on incentive mechanisms for DTN with nodes' selfishness," *IEEE Access*, vol. 6, pp. 29 419–29 425, 2018. [Online]. Available: https://doi.org/10.1109/ACCESS.2018.2834912

[13] A. Chhabra, V. Vashishth, and D. K. Sharma, "SEIR: A stackelberg game based approach for energy-aware and incentivized routing in selfish opportunistic networks," in *51st Annual Conference on Information Sciences and Systems, CISS 2017, Baltimore, MD, USA, March 22-24, 2017*. IEEE, 2017, pp. 1–6. [Online]. Available: https://doi.org/10.1109/CISS.2017.7926113

[14] L. Li, Y. Qin, X. Zhong, and H. Chen, "An incentive aware routing for selfish opportunistic networks: A game theoretic approach," in *8th International Conference on Wireless Communications & Signal Processing, WCSP 2016, Yangzhou, China, October 13-15, 2016*. IEEE, 2016, pp. 1–5. [Online]. Available: https://doi.org/10.1109/WCSP.2016.7752714

[15] Y. Cai, Y. Fan, and D. Wen, "An incentive-compatible routing protocol for two-hop delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 266–277, 2016. [Online]. Available: https://doi.org/10.1109/TVT.2015.2454291

[16] K. Chen, H. Shen, and L. Yan, "Multicent: A multifunctional incentive scheme adaptive to diverse performance objectives for DTN routing," *IEEE Trans. Parallel Distributed Syst.*, vol. 26, no. 6, pp. 1643–1653, 2015. [Online]. Available: https://doi.org/10.1109/TPDS.2014.2323057

[17] Y. Mao and P. Zhu, "A game theoretical model for energy-aware DTN routing in manets with nodes' selfishness," *Mob. Networks Appl.*, vol. 20, no. 5, pp. 593–603, 2015. [Online]. Available: https://doi.org/10.1007/s11036-015-0610-7

[18] J. Wu, Y. Zhu, L. Liu, B. Yu, and J. Pan, "Energy-efficient routing in multi-community DTN with social selfishness considerations," in *2016 IEEE Global Communications Conference, GLOBECOM 2016, Washington, DC, USA, December 4-8, 2016*. IEEE, 2016, pp. 1–7. [Online]. Available: https://doi.org/10.1109/GLOCOM.2016.7841809

[19] F. Lu, J. Li, S. Jiang, Y. Song, and F. Wang, "Geographic information and node selfish-based routing algorithm for delay tolerant networks," *Tsinghua Science and Technology*, vol. 22, no. 3, pp. 243–253, 2017.

[20] Y. Wu, S. Deng, and H. Huang, "Control of message transmission in delay/disruption tolerant network," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 1, pp. 132–143, 2018.

[21] X. Zhang, G. Neglia, J. F. Kurose, and D. F. Towsley, "Performance modeling of epidemic routing," *Comput. Networks*, vol. 51, no. 10, pp. 2867–2891, 2007.